PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-212356
(43)Date of publication of application : 11.08.1995

(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00

(21)Application number : 06-278074
(22)Date of filing : 11.11.1994

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : ROGAWAY PHILLIP W

(30)Priority
Priority number : 93 175881 Priority date : 30.12.1993 Priority country : US

(54) METHOD AND SYSTEM FOR AUTHENTICATING COMMUNICATION PARTNER

(57)Abstract:
PURPOSE: To protect an information stream from hostile persons.
CONSTITUTION: In a method for authenticating communication partners, entity authenticating operations and temporary secret key distributing operations are nearly simultaneously executed through an unstable communication channel between communication partners. In this method, the authenticity of the communication partners is discriminated by the possession of a permanent shared secret key. This method includes several steps. To define a composite key, a data flow is exchanged between the communication partners. At least a portion of the data flow is encrypted so that the permanent secret key may be used or masked. At least one authentication tag is exchanged between the communication partners through the communication channel. At least part of at least one authentication tag is based on the composite key. The authentication tag is used to discriminate the authentication of at least one communication partner.

LEGAL STATUS

[Date of request for examination]	11.11.1994
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2926699
[Date of registration]	14.05.1999
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	14.05.2004

(19)日本国特許庁(JP)　(12)特許公報（Ｂ２）　(11)特許番号

第２９２６６９９号

(45)発行日　平成11年(1999)7月28日　(24)登録日　平成11年(1999)5月14日

(51)Int. Cl.[6]	識別記号	FI		
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ	9/00	６７３　Ａ
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ	1/00	６３０　Ｃ
				６３０　Ｅ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ	9/00	６０１　Ｃ
				６０１　Ｅ

請求項の数１８　(全１１頁)

(21)出願番号　特願平6-278074

(22)出願日　平成6年(1994)11月11日

(65)公開番号　特開平7-212356

(43)公開日　平成7年(1995)8月11日

審査請求日　平成6年(1994)11月11日

(31)優先権主張番号　175881

(32)優先日　1993年12月30日

(33)優先権主張国　米国（ＵＳ）

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(74)代理人　弁理士　坂口　博　（外1名）

審査官　松尾　淳一

最終頁に続く

(54)【発明の名称】通信パートナの認証方法及びシステム

(57)【特許請求の範囲】

【請求項１】安全でない通信チャネルの通信パートナの信憑性を永続的な共用秘密キーの所有によって判別する、通信パートナを認証する方法において、

（ａ）第１の要素及び第２の要素によって規定される複合キーの第１の要素を前記永続的な共用秘密キーにより暗号化したもの、及び第１のテキスト・データを含むデータ流を第１の通信パートナから第２の通信パートナに通信するステップと、

（ｂ）前記第１の通信パートナから第２の通信パートナへの通信に応答して、前記複合キーの第２の要素を前記永続的な共用秘密キーにより暗号化したもの，及び前記第１の通信パートナから第２の通信パートナに通信されたデータ流を前記永続的な共用秘密キーにより変換したものを含むデータ流を第２の通信パートナから第１の通

信パートナに通信するステップと、

（ｃ）前記第２の通信パートナから第１の通信パートナに通信されたデータ流を使用して、前記第２の通信パートナの信憑性及び前記第１のテキスト・データの認証を前記第１の通信パートナにおいて判別するステップと、を含む方法。

【請求項２】前記複合キーの第１の要素は指数関数の第１の指数要素であり、

前記複合キーの第２の要素は指数関数の第２の指数要素である、

ことを特徴とする請求項１に記載の通信パートナを認証する方法。

【請求項３】前記第１の指数要素が、公知の基数と、前記第１の通信パートナが事前に定義された整数群から選択した任意の秘密の指数とを含むことを特徴とする、請

求項２に記載の通信パートナを認証する方法。

【請求項４】前記第２の指数要素が、公知の基数と、前記第２の通信パートナが事前に定義された整数群から選択した任意の秘密の指数とを含むことを特徴とする、請求項３に記載の通信パートナを認証する方法。

【請求項５】（ｄ）第２の通信パートナから第１の通信パートナに通信されるデータ流が第２のテキスト・データを含み、

（ｅ）第２の通信パートナから第１の通信パートナに通信されるデータ流に応答して、第３のテキスト・データと、該第３のテキスト・データ及び前記複合キーを前記永続的な共用秘密キーにより暗号化したものを含むデータ流を第１の通信パートナから第２の通信パートナに通信する前記第１の通信パートナにある手段を更に含む事を特徴とする請求項１に記載の通信パートナを認証する方法。

【請求項６】前記複合キーがｇのαβ乗で表され、

第１の通信パートナのために、特定のｇ及び事前に定義された群から秘密に選択されたαの値からｇのα乗の値を計算するサブステップと、

第２の通信パートナのために、前記特定のｇ及び事前に定義された群から秘密に選択されたβの値からｇのβ乗の値を計算するサブステップと、

前記安全でない通信チャネルを介して前記第１および第２の通信パートナ間で行われる通信を保護する場合に一時的な共用秘密キーとしての複合キーであるｇのαβ乗を生成するサブステップとを含む、請求項２に記載の通信パートナを認証する方法。

【請求項７】前記複合キーの一部がｇのα乗で表され、

永続的な共用秘密キーを用いて前記ｇのα乗の値を変換するサブステップと、

前記複合キーの別の一部がｇのβ乗で表され、永続的な共用秘密キーを用いて前記ｇのβ乗の値を変換するサブステップと、

を含む、請求項１に記載の通信パートナを認証する方法。

【請求項８】前記変換が排他的論理和演算を含む、請求項７に記載の通信パートナを認証する方法。

【請求項９】前記変換が暗号化演算を含む、請求項７に記載の通信パートナを認証する方法。

【請求項１０】安全でない通信チャネルの通信パートナの信憑性を永続的な共用秘密キーの所有によって判別する、第１の通信パートナと第２の通信パートナとの間で通信パートナを認証するシステムにおいて、

（ａ）第１の要素及び第２の要素によって規定される複合キーの第１の要素を前記永続的な共用秘密キーにより暗号化したもの、及び第１のテキスト・データを含むデータ流を第１の通信パートナから第２の通信パートナに通信する前記第１通信パートナにある手段と、

（ｂ）前記第１の通信パートナから第２の通信パートナへの通信に応答して、前記複合キーの第２の要素を前記永続的な共用秘密キーにより暗号化したもの，及び前記第１の通信パートナから第２の通信パートナに通信されたデータ流を前記永続的な共用秘密キーにより変換したものを含むデータ流を第２の通信パートナから第１の通信パートナに通信する前記第２通信パートナにある手段と、

（ｃ）前記第２の通信パートナから第１の通信パートナに通信されたデータ流を使用して、前記第２の通信パートナの信憑性及び前記第１のテキスト・データの認証を前記第１の通信パートナにおいて判別する前記第１通信パートナにある手段と、

を含むシステム。

【請求項１１】前記複合キーの第１の要素は指数関数の第１の指数要素であり、

前記複合キーの第２の要素は指数関数の第２の指数要素である、

ことを特徴とする請求項１０に記載の通信パートナを認証するシステム。

【請求項１２】前記第１の指数要素が、公知の基数と、前記第１の通信パートナが事前に定義された整数群から選択した任意の秘密の指数とを含むことを特徴とする、請求項１１に記載の通信パートナを認証するシステム。

【請求項１３】前記第２の指数要素が、公知の基数と、前記第２の通信パートナが事前に定義された整数群から選択した任意の秘密の指数とを含むことを特徴とする、請求項１２に記載の通信パートナを認証するシステム。

【請求項１４】（ｄ）第２の通信パートナから第１の通信パートナに通信されるデータ流が第２のテキスト・データを含み、

（ｅ）第２の通信パートナから第１の通信パートナに通信されるデータ流に応答して、第３のテキスト・データと、該第３のテキスト・データ及び前記複合キーを前記永続的な共用秘密キーにより暗号化したものを含むデータ流を第１の通信パートナから第２の通信パートナに通信する前記第１の通信パートナにある手段を更に含む事を特徴とする請求項１０に記載の通信パートナを認証するシステム。

【請求項１５】前記複合キーがｇのαβ乗で表され、

第１の通信パートナのために、特定のｇ及び事前に定義された群から秘密に選択されたαの値からｇのα乗の値を計算する前記第１の通信パートナにある手段と、

第２の通信パートナのために、前記特定のｇ及び事前に定義された群から秘密に選択されたβの値からｇのβ乗の値を計算する前記第２の通信パートナにある手段と、

前記安全でない通信チャネルを介して前記第１および第２の通信パートナ間で行われる通信を保護する場合に一時的な共用秘密キーとしての複合キーであるｇのαβ乗を生成する前記第１の通信パートナにある手段とを含む、請求項１１に記載の通信パートナを認証するシステ

ム。

【請求項１６】前記複合キーの一部がｇのα乗で表され、永続的な共用秘密キーを用いて前記ｇのα乗の値を変換する前記第１の通信パートナにある手段と、

前記複合キーの別の一部がｇのβ乗で表され、永続的な共用秘密キーを用いて前記ｇのβ乗の値を変換する前記第２の通信パートナにある手段と、

を含む、請求項１０に記載の通信パートナを認証するシステム。

【請求項１７】前記変換が排他的論理和演算を含む、請求項１６に記載の通信パートナを認証するシステム。

【請求項１８】前記変換が暗号化演算を含む、請求項１６に記載の通信パートナを認証するシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、一般的には情報の流れを敵対者から保護するための方法に関し、より具体的には、通信パートナの身元を検査し、複数の通信パートナ間でセッション・キーを分配するための方法に関する。

【０００２】

【従来の技術】分散データ処理システムを使用して、機密情報を共用し、やりとりする機会が増しているため、コンピュータ業界および関連業界は、電話回線などの安全でない通信チャネルおよびセルラー・ネットワークなどの電磁方式の通信システムを介してやりとりされるデータを保護するための既知の方法の改善および向上にさらに多くの注意を払っている。

【０００３】長年に渡り業界が目標としてきたものは３つある。まず１つ目として、分散データ処理システム内の特定の通信パートナが、分散データ処理システム内の他の通信パートナの身元を認証できることが重要である。一般に、このエンティティ認証要件は、データ処理システム内の２つまたはそれ以上の通信ノードに永続的な（long-lived）共用秘密キーを置くことによって満たされる。たとえば、ユーザは、データ処理システム内のホスト・コンピュータも把握している秘密のパスワードを所有することができる。認証が必要な場合は、この共用秘密キーに基づいて一方の当事者をもう一方の当事者に対して認証するか、あるいはそれぞれの当事者を残りの当事者に対して認証するためのプロトコルが実行される。たとえば、ＤＥＳ暗号化などの従来の暗号化動作では、この永続的な共用秘密キーを使用することができる。最も一般的なのは、もう一方の通信パートナの認証を希望する通信パートナが、ランダム・ビット・ストリームの形式になっている「識別要求（challenge）」をもう一方の通信パートナに送る方法である。認証の対象となるパートナは、通常、永続的な共用秘密キーを使ってこの識別要求ビット・ストリームに対して暗号化動作を実行してから、このデータを要求側に返す。このデータは解読されて、応答側が永続的な共用秘密キーを所有

しているかまたはそれを知っているかどうか、あるいは、求めている応答を生成し、正しい回答に対する応答を圧縮するための暗号化エンジンを要求側が使用しているかどうかを判別する。このような認証動作は、一方的に行うか、相互に行うことができる。一方的な動作の場合は、一方の当事者が分散データ処理システム内のもう一方の当事者の身元の認証を取得する。相互エンティティ認証手順の場合は、通常、両方の当事者が相手側に対して「識別要求」を出すが、この識別要求に対して正しく応答しないと、通信ノード間の通信が可能にならない。

【０００４】業界の２つ目の目標は、様々な通信パートナすべての認証を取得した後で分散データ処理システム内の２人またはそれ以上の通信パートナが共用する、一時的な（short-lived）秘密セッション・キーを生成して分配するための方法を提供することである。本発明によれば、一時的な秘密セッション・キーの分配は、エンティティ認証動作と緊密に結び付いている。セッション・キーを使用すると、絶対的に必要な回数を上回るほど永続的な共用秘密キーを使用する必要がなくなり、通信パートナが関与する通信セッションで「再生攻撃（replay attack）」から保護することがさらに有効であることを保証する。一般に、永続的な共用秘密キーの使用は、エンティティ認証動作中に限られる。通信当事者の認証の取得後、ただちに一時的な秘密セッション・キーが分配され、特定のセッションの当事者間の通信に対して認証または暗号化あるいはその両方を実行できるようにするためにそのキーが使用される。

【０００５】業界の３つ目の目標は、安全でない回線を介してデータを受け取った通信当事者に対し、伝送中にそのデータが変更されていないことを保証することである。多くの場合、このようなメッセージ認証は、送信するメッセージと通信パートナ間で共用される秘密キーとの関数として短い「認証タグ」を発信側が計算することによって行っている。この認証タグは、通常、当事者間でやりとりされるデータ・ストリームに付加される。データ・ストリームと認証タグを受け取ると、受信側は、独自の認証タグを生成するために送信側がデータ・セットに対して行ったのと同じ動作を行うことで、認証タグを分析する。送信側の認証タグが受信側が認証したタグと完全に一致すると、データの受信側は、そのデータが一切変更されていないという保証が得られる。この種の保護対策は、活動的な敵対者（adversary）が安全でない通信チャネルに入り込んで、データを改ざんするのを防止するものである。

【０００６】通信パートナ間の安全な通信を可能にするためのセキュリティ・システムを考案する場合、一般に、敵対者は、（１）受動的で、分散データ処理システム内の当事者間のすべての通信を監視して記録するために盗聴作業を行うか、（２）活動的で、データまたは資

源へのアクセスを要求して、認証用の識別要求を発行したり、それに応答することで、分散データ処理システム内の通信に実際に参加する可能性があるものとして想定される。活動的な敵対者の能力は、受動的な敵対者の能力すべてを含むものと見なされる。企図されるある種の敵対攻撃（attack）は、監視および記録活動を行う初期の受動期間と、それに続いて、監視活動中に入手したデータをオフラインで分析して操作する期間、さらにそれに続いて、データおよびデータ処理資源へのアクセスを要求する短い間隔の活動で構成される。あるいは、敵対者は、単に受動的な監視および記録活動に関与し、その後、分析し、データの各部分を暗号解読する試み、特に、セッション・キーを回復する試みを行うだけの可能性があるが、回復したセッション・キーは、当事者間で送信され、敵対者が記録した暗号化データの解読に使用される。

【０００７】監視、記録、およびその後のオフライン分析を行うだけの受動的な敵対者は、１人または複数の許可通信当事者と対話せざるを得ない活動的な敵対者に比べ、検出するのが難しいので、敵対者は受動的な攻撃を好む。敵対者がオフライン分析の方を好むさらに重要な理由は、通信チャネルに存在する帯域制限である。つまり、敵対者は、システム体系によって定義され許可されている速度でしか通信パートナに話しかけることができないが、オフライン分析は、敵対者のコンピューティング資源の速度で実行することができる。したがって、敵対者が受動的な活動中に有効なデータを収集するのを防止できるデータ・セキュリティ・システムを提供することが特に重要である。また、永続的な共用秘密キーだけでなく、使われた可能性のある一時的な秘密セッション・キーについても被害を防止できるようにセキュリティ・システムを設計することが特に重要である。セキュリティ・システムは、受動的な敵対者がオフライン分析中に永続的または一時的なキーを正確に推測し、それからオフライン活動中にその推測の正確さを確認するのを防止できることが特に重要である。正確に推測したキーの正確さを確認するためには、敵対者は１人または複数の通信当事者と積極的に関わらざるを得ないことが重要である。この種の保護対策は、「オフライン攻撃からの保護」と呼ばれるもので、「辞書攻撃（dictionary attack）」と呼ばれるある種のオフライン攻撃の具体的な例の場合に最もよく理解することができる。「辞書攻撃」については、後述する。

【０００８】辞書攻撃が効果的である理由は、エンティティ認証に使用する永続的なキーがユーザのパスワードに基づくもので、これらのパスワードの選び方が不適切な場合がよくあるためである。多くのデータ処理システムは、オペレータが自分のパスワードを選択できるようになっている。後でパスワードを思い出しやすくするため、ありふれた単語を選んでしまうのは当然のことである。ユーザが固有の名前または普通名詞または動詞をパスワードとして使用することは、まれなことではない。言語はかなり小さな固定集合なので、受動的な敵対者が、１つまたは複数の特定の言語からなる候補を反復して推測し、盗聴活動中に以前のセッションで記録したトランスクリプトをこのような推測が「説明している」かどうかを判断することは可能である。一致が判明すると、通常、正確なパスワードに基づいて分配が行われる一時的なキーのようにこのパスワードが回復される。当然、辞書のサイズが非常に大きければ、この種のオフライン攻撃がコンピュータ使用の上で大変な労力を要する場合もあり得るが、処理速度や能力が継続的に大幅に進歩しているため、この辞書に膨大な数の単語が収容されていても、このようなオフライン攻撃が実際的である。

【０００９】

【発明が解決しようとする課題】本発明の一目的は、敵対者が候補となるキーについて行う上記の推測ごとにその正確さを１人または複数の通信当事者との対話により確認せざるを得ないようにすることで、辞書攻撃などのオフライン攻撃の影響を受けにくい、セキュリティ・システムを提供することである。

【００１０】本発明の他の目的は、エンティティ認証動作およびキー分配時に通信当事者間でやりとりしなければならない通信の流れの数を最小限にする、セキュリティ・システムを提供することである。

【００１１】本発明の他の目的は、先行技術による既存のセキュリティ・システムに比べ、暗号化動作および解読動作への依存度が低く、システム・セキュリティを最大化するために、永続的な共用秘密キーまたはその派生物を含む複数のパラメータに適用されるメッセージ認証コードや暗号化ハッシュ関数などの変換への依存度がかなり高い、セキュリティ・システムを提供することである。

【００１２】本発明の他の目的は、ＤＥＳアルゴリズムなどの暗号化技術を従来通り利用する代わりに、エンティティ認証を行うために永続的な共用秘密キーまたはその派生物を含む複数のパラメータに適用される１つまたは複数のコンピュータによる不可逆性の変換を利用する、セキュリティ・システムを提供することである。実施例では、この種の認証タグ方式のエンティティ認証を指数キー交換と組み合わせて使用する。本方法は、２人または３人の当事者を含む、一方的または多角的な認証の実行に使用することができる。

【００１３】

【課題を解決するための手段】上記およびその他の目的は、以下に説明するように達成される。永続的な共用秘密キーを所有していることによって通信パートナの信憑性が判別される、安全でない通信チャネルでの通信パートナを認証するための方法を提供する。本方法はいくつかのステップを含む。最初のステップでは、通信パート

ナ間のデータの流れで「複合キー」が交換されるが、データの流れの少なくとも一部は、永続的な共用秘密キーを使用できるように、暗号化されるか、その他の方法でマスキングされている。次のステップでは、少なくとも１つの認証タグが通信パートナ間でやりとりされるが、少なくとも１つの認証タグは、少なくとも部分的に複合キーに基づくものである。最後のステップでは、少なくとも一方の通信パートナが認証タグを使用して、もう一方の通信パートナの信憑性を判別する。本発明の実施例では、少なくとも１つの認証タグは、（１）前記永続的な共用秘密キーによって複数のパラメータを変換して生成されるメッセージ認証コード、（２）永続的な共用秘密キーおよび複数のその他のパラメータに対して適用される暗号ハッシュ関数、および（３）前記永続的なキーによって変換され、複数のパラメータの暗号ハッシュを介して生成される暗号化またはメッセージ認証コードのうちの少なくとも１つを含む変換によって定義される。第１の当事者と第２の当事者間で相互認証が必要な、本発明の特定の実施例では、両当事者は、まず従来の秘密キー交換を使用して複合キーの部分を交換する。ただし、米国特許第４２４１５９９号に記載されるように、この交換の流れの一部または全部が暗号化される。次に、第１および第２の通信当事者間で第１および第２の認証タグが交換される。この認証タグは、第１および第２の通信パートナのエンティティ認証を行うために分析される。本発明の具体的な一実施例では、第１および第２の通信パートナ間の通信の流れの数を最小限にするため、第１および第２の認証タグの少なくとも１つが、複合セッション・キーの少なくとも一部とともに、第１および第２の通信パートナ間でやりとりされる。本発明の特定の実施例では、新たに分配したセッション・キーを含む複数のパラメータにハッシュ関数を適用し、このハッシュ関数の接頭部を認証タグとして使用することで認証タグを生成する。

【００１４】要約すると、本発明で提示されるのは、通信パートナ間の安全でない通信チャネルを介して、エンティティ認証動作と一時的な秘密キーの分配動作をほぼ同時に実行するための方法である。この方法では、通信パートナの信憑性は、永続的な共用秘密キーの所有によって判別される。本方法は、いくつかのステップを含む。複合キーを定義するために、通信パートナ間でデータの流れが交換される。データの流れの少なくとも一部は、永続的な共用秘密キーを使用できるように暗号化されているか、あるいはマスキングされている。少なくとも１つの認証タグが、通信チャネルを介して通信パートナ間でやりとりされる。少なくとも１つの認証タグは、その少なくとも一部が複合キーに基づくものである。認証タグは、少なくとも一方の通信パートナの信憑性を判別するために使用される。分散データ処理システムにおける主な商用応用例の１つを参照して本発明を説明するが、本発明は汎用性のあるもので、考えられるどのような通信チャネルでメッセージをやりとりする場合にも使用でき、特に秘話通信に有効であることは明らかである。

【００１５】

【実施例】図１、図２、および図３は、データのやりとりを保護するための先行技術を示す図である。これらの先行技術を理解すると、図４および図５に示す本発明の実施例が理解しやすくなる。

【００１６】図１には、先行技術による３パス・メッセージ認証方法を示す。図示の通り、ＡおよびＢは通信パートナで、永続的な共用秘密キーａを共用している。通信パートナＡおよびＢは、安全でない（insecure）通信チャネルを介して通信する。図１には３つのデータの流れが示されている。第１のデータの流れは、通信パートナＡから通信パートナＢに送られるもので、エンティティ認証識別要求を表すランダム・ビット・ストリングR_Aを含む。第１のデータの流れは、任意のテキスト・ストリングＴｅｘｔ１も含む。通信パートナＢは、ランダム・ビット・ストリングR_B、任意のテキスト・ストリングＴｅｘｔ２、および変換h^1の結果であるビット・ストリングを通信パートナＡに送ることによって、第１の通信の流れに応答する。この変換h^1は、変換キーとして永続的な共用秘密キーａを使用し、通信パートナＡおよびＢの識別コード、通信パートナＡおよびＢによって生成された認証識別要求R_AおよびR_B、ならびにテキスト・ストリングＴｅｘｔ１およびＴｅｘｔ２を含む複数のデータ項目に適用される。

【００１７】通信パートナＡは永続的な共用秘密キーａを所有しているので、パートナＡは、変換h_a^1を使用した結果として通信パートナＢが提供するものと同一の（第２の流れが正しく計算され、送信したとおりに受信される場合）ビット・ストリームを生成するために、通信パートナＢからの認証識別要求R_Bを使用することができる。通信パートナＢが、通信パートナＡが生成したものと同一であるビット・ストリームを変換h_a^1を使用して生成するには、永続的な共用秘密キーを所有していることが必要なので、通信の流れ２の終了時に、通信パートナＡは通信パートナＢが「本物」であることを確認できる。

【００１８】第３の通信の流れでは、通信パートナＡが、Ｔｅｘｔ３と、認証識別要求R_BおよびＴｅｘｔ３に変換h_a^2を適用した結果とを送出する。通信パートナＢは、通信パートナＡが提供するものに匹敵するビット・ストリームを生成するために、永続的な共用秘密キーａ、認証識別要求R_B、Ｔｅｘｔ３、および変換h^2を使用することができる。両方のビット・ストリームが同じであれば、通信パートナＢは、通信パートナＡが「本物」であることを確認できる。図１に示した方法は、M. BellareおよびP. Rogawayによる"Entity Authenticati

on and Key Distribution" (Springer-VerlagによってThe Proceeding of Crypto '93で発表) でさらに詳しく論じられている。基本的に、図１の方法では、従来のエンティティ認証識別要求方法が、従来のメッセージ認証方法と組み合わせて使用されている。

【００１９】図２は、"New Directions in Cryptography" (IEEE Transactions On Information Theory, IT-22, No.6, 1976) という論文に記載された、W. DiffieおよびM. Hellmanの教示による従来のキー交換を示している。この方法は、具体的にはDiffie-Hellmanキー交換と呼ばれる場合もある。この方法の目的は、特定の通信セッションに使用できる共用秘密キーを生成するために結合できる情報を公に交換することである。このプロトコルによれば、通信パートナＡは、一定の素数ｐの乗法群モジュロなどの公知のベキ数群から秘密に選択されたベキ数αで公知の基数ｇを累乗することによって生成したビット・ストリームを通信パートナＢに送る。通信パートナＢは、αが選択されたのと同じ公知のベキ数群から秘かに選択したベキ数βで公知の基数ｇを累乗することによって生成したビット・ストリームを通信パートナＡに送ることで、通信の流れ２で応答する。共用秘密キーσは、上記２つの通信の流れで通信パートナＡとＢとの間でやりとりされる情報を使用して生成される。図２に示すように、共用秘密キーσは、ｇのα乗とｇのβ乗との指数積に適用される変換H_1の関数である。αおよびβの値は、事前に定義された一連の整数から通信パートナＡおよびＢが任意に選択したものであることが好ましい。

【００２０】Diffie-Hellmanキー交換は、受動的な敵対者の影響を受ける可能性があるが、活動的な敵対者の影響を受けない通信チャネルでのみ有効である。つまり、通信チャネルが敵対者による対話の影響を受けやすい場合、敵対者は、通信パートナＡまたはＢを装い、許可を受けた当事者から情報を入手するのに使用できる共用秘密キーの生成を開始することができるので、Diffie-Hellmanキー交換プロトコルはあまり有効ではない。

【００２１】図２のDiffie-Hellmanキー交換プロトコルのような従来のキー交換方法は、BellovinおよびMerrittによって"Encrypted Key Exchange: Password Based Protocol Secure Against Dictionary Attacks" (IEEE Symposium On Research And Security And Privacy, 1992の議事録に掲載) という論文に詳しく述べられていると同時に、米国特許第５２４１５９９号の主題でもある。BellovinおよびMerrittの方法の裏にある広い概念は、図３に示されている。図示の通り、通信パートナＡおよびＢは永続的な秘密キーａを共用する。図３には２つの通信の流れが示されているが、さらに通信の流れを追加することも可能である。第１の通信の流れでは、通信パートナＡは、公知の基数ｇに対して、任意に選択された秘密キーα（一定の基礎群から拾った認証キー）を

指数として適用し、永続的な共用秘密キーａを用いるマスキング変換E_a^1でｇのα乗を表すビット・ストリームを暗号化する。第２の通信の流れでは、通信パートナＢは、基数ｇに対して、任意に選択された秘密キーβを指数として適用し、ｇのβ乗によって生成されたビット・ストリームに対し、変換E_a^2を適用することで応答している。この方法によれば、この対話の結果として生成されたキーは、特定の関数H_1の場合のH_1（ｇのαβ乗）に等しいσになる。このプロトコルでは、変換E^1およびE^2は排他的論理和演算またはその他のマスキング演算にすることができる。この方法を使用して、BellovinおよびMerrittは、Diffie-Hellmanキー交換により、活動的な敵対者と受動的な敵対者のどちらについても安全な一時的なセッション・キーを定期的に生成するのに使用できるプロトコルを考案した。交換するデータが、永続的な共用秘密キーａを変換キーとして用いる変換によって暗号化され、その結果、辞書攻撃などの受動的なオフライン攻撃の影響を受けなくなるため、通信の流れ１および２に含まれる情報は盗聴の影響を受けない。

【００２２】本発明の一実施例について、図４を参照して説明する。本発明は、以下の結果を同時に得るのに使用できるセキュリティ・プロトコルを提示する。その結果とは、（１）通信システムにおいて２人またはそれ以上の当事者間のエンティティ認証に対応すること、（２）通信システムにおいて当事者間でやりとりされるメッセージのエンティティ認証を達成するために、暗号化の代わりにタグを使用すること、（３）通信システム内の２人またはそれ以上の当事者が一時的なセッション・キーを分配できるようにすること、（４）エンティティ認証およびセッション・キーの分配の目的が、通信システム内の複数の当事者間の最低数の通信の流れで達成され、特に、それぞれの特定のデータの流れでエンティティ認証とキー分配という目標をほぼ同時に追求することによって達成されること、（５）通信システムがオフライン攻撃に対して安全で、特に、辞書攻撃に対して安全であること、および（６）敵対者が永続的なキーの知識を利用して記録したセッションの機密性に害を及ぼさないようにする、セキュリティ・システムの完璧で前向きな機密性を提供することである。

【００２３】図４に示すように、この実施例では、永続的な秘密キーａを共用する通信パートナＡおよびＢの間に３つの連続するデータの流れが必要であるが、代替実施例では、データの流れの特定部分を個別の通信用に分離することで、さらに多くのデータの流れ、たとえば、４つまたは５つのデータの流れで本発明の諸目的を達成できるはずである。

【００２４】図４のシナリオでは、通信パートナＡは通信パートナＢにＴｅｘｔ１を渡そうとしている。通信パートナＢは、通信パートナＡにＴｅｘｔ２を送ることで応答する。次に通信パートナＡは、通信パートナＢにＴ

ｅｘｔ３を送ることで通信パートナＢに応答する。このデータ交換の間、通信パートナＡおよびＢは、それぞれの通信が「本物」の発信源によって生成されていることと、テキスト・メッセージまたはデータが敵対者によって一切変更されていないことを確認したいと考えている。また、これらの通信パートナは、その後のメッセージ認証または暗号化あるいはその両方に使用する最新のセッション・キーを分配したいと考えている。このような目標を達成するため、第１の通信の流れで通信パートナＡは、Ｔｅｘｔ１とともに、暗号化またはその他の方法でマスキングを行ったビット・ストリームを通信パートナＢに送る。より具体的には、通信パートナＡは、図２に示した前述のDiffie-Hellmanキー交換により、αを選択する。αは、モジュルｐの整数の乗法的群から０及びｐ－２の間で任意に選択する。任意に選択したαを公知の基数ｇに指数として適用し、数値ｇのα乗に対して変換E^1を行う。この変換E^1は、永続的な共用秘密キーａを変換キーとして用い、ｇのα乗と永続的な共用秘密キーａとを使用して行う排他的論路和演算を含むことができる。通信の流れでは、この動作はE_a^1として表される。したがって、従来の秘密キー交換の第１の流れに対して変換E_a^1によるマスキングが行われる。

【００２５】第２の通信の流れでは、通信パートナＢは、テキスト部分Ｔｅｘｔ２と、２つのその他の構成要素を通信パートナＡに送る。第１の構成要素は、Diffie-Hellmanキー交換モデルなどの従来のキー交換の第２の流れである。より具体的には、通信パートナＢは、αが選択された整数の組から任意のβを選択する。任意に選択したβを公知の基数ｇに指数として適用する。数値ｇのβ乗については、永続的な共用秘密キーａを変換キーとして用い、その結果、通信の流れ２でE_a^2として表される変換E^2を行うことができる。第２の構成要素は、マスキング変換h^1を適用した結果である。このマスキング変換h^1は、永続的な共用秘密キーａを変換キーとして用い、通信パートナＢの識別コード、通信パートナＡの識別コード、第１のデータの流れで送信されたテキスト部分Ｔｅｘｔ１、第２のデータの流れで送信されたテキスト部分Ｔｅｘｔ２、およびE_a^1（ｇのα乗）とE_a^2（ｇのβ乗）の変換を含む複数のパラメータに適用される。さらに、σも変換h_a^1の対象になるが、σは、図２のDiffie-Hellmanプロトコルにより、ｇのαβ乗モジュロｐとして定義される。

【００２６】このようにして、最初の２つの通信の流れでは、通信パートナＡおよびＢが、２つのテキスト部分だけでなく、σとして定義された一時的な（セッション）キーを共同定義する２つの流れも交換する。ただし、このキーの流れは、永続的な共用秘密キーａにアクセスできない敵対者にとって役に立たないものになるように暗号化が行われている。第２の通信の流れでは、変換h_a^1によって生成されたビット・ストリームが２重の

機能を果たしている。１つは、Ｔｅｘｔ１とＴｅｘｔ２のデータに対してメッセージ認証手順を実行することで、もう１つは、（σまたはａを含むパラメータ群に暗号化変換h^1を適用することで）通信パートナＡに対して通信パートナＢが本物であると認証することである。

【００２７】第３の通信の流れでは、テキスト部分Ｔｅｘｔ３が通信パートナＡから通信パートナＢに送信される。さらに、暗号変換h^2は、永続的な共用秘密キーａを変換キーとして用い、E_a^2により変換が行われる変換済みの複合キー部分ｇのβ乗、テキスト部分Ｔｅｘｔ３、およびセッション・キーを表すσを含む、少なくとも３つのパラメータに適用される。この第３の通信の流れの結果、通信パートナＡは、暗号化変換h_a^2が行われるパラメータにσを含めることで、自分自身が本物であることを通信パートナＢに対して認証している。同時に、変換h_a^2がメッセージ認証変換として機能するので、Ｔｅｘｔ３に含まれるデータの正確さが保証される。

【００２８】本発明の実施例では、変換E^1、E^2、h^1、およびh^2の暗号化または暗号変換関数を実行するために、複数の従来の変換を使用することができる。たとえば、暗号化または暗号変換E_a^1では、ｇのα乗に対する永続的な共用秘密キーａの排他的論理和を取ることができる。ビット・ストリームｇのβ乗に対する永続的な共用秘密キーａの排他的論理和は、暗号変換E^2として使用することができるはずである。

【００２９】本発明によれば、暗号化またはマスキング変換h^1およびh^2は、（１）永続的な共用秘密キーａを変換キーとして用い、σまたは複合キー部分を含む複数のパラメータに適用されるメッセージ認証コード演算、または（２）永続的な共用秘密キーａを変換キーとして用い、複合セッション・キーσまたは複合セッション・キーの一部を含む複数のパラメータに適用される暗号ハッシュ関数、または（３）永続的なキーａを変換キーとして用い、複数のパラメータの暗号ハッシュに対して生成される暗号化またはメッセージ認証コードのいずれかであることが好ましい。

【００３０】本発明の実施例では、変換h_a^1およびh_a^2は、従来のメッセージ認証コード方法または従来のハッシュ関数のいずれかである。メッセージ認証コード演算の目的を達成するための機構は数多く存在するが、主な機構は以下のものを含む。

（１）″ＣＢＣ$_a$Ｃ（ｘ）″として表される、永続的な秘密キーａの下で特定のビット・ストリームのブロック暗号α（すなわち、暗号ブロック連鎖）を使用したＣＢＣ暗号の最後のワードの接頭部

（２）″hash（ｘ，ａ）″として表される、特定のビット・ストリームと永続的な共用秘密キーａとの暗号ハッシュの接頭部

（３）″ＣＢＣ$_a$（hash（ｘ，ａ））″として表され、上

記の演算（２）の暗号ハッシュ関数について行われる暗号ブロック連鎖演算の接頭部を生成する上記（１）の演算と（２）の演算の組合せ

（４）"Encryption（hash（ｘ））"として表すことができる、ハッシュ演算と暗号化演算（ＤＥＳアルゴリズムなど）の組合せ。

【００３１】メッセージ認証コード演算

メッセージ認証コード（Message Authentication Code：ＭＡＣ）は、通信の信憑性を保証するために暗号化で使用される。このようなタイプの演算は、「メッセージ認証演算」と呼ばれることが多い。通常、メッセージ認証演算によって、受信側は、メッセージの発信元と宛先、内容、適時性、通信者間でやりとりされる他のメッセージとの相対的な順序を確認することができる。

【００３２】メッセージ認証コード（ＭＡＣ）演算を実行するために様々なアルゴリズムを使用することができるが、最もよく知られている正式体系はDES MODES OF OPERATION、より具体的には、１９８０年１２月２日にNational Bureau of Standardsから発行されたFederal Information Processing Standards Publication, FIPSPUB 81に記載されている。暗号ブロック連鎖（Cipher Block Chaining：ＣＢＣ）モードは、非暗号テキストを暗号化するのに使用することが好ましいが、この非暗号化テキストは、長さが６４ビットの倍数であることが必要な場合は（ゼロ・ビットなどで）埋込みを行わなければならない。ＭＡＣは、暗号テキストの最後のｋビットで構成され、残りのビットは破棄される。このプロセスは、C. H. MeyerおよびS. M. Matyasによる"Cryptography: A New Dimension in ComputerData Security"（John Wiley & Sons, New York, 1982）という論文で論じられている。暗号ブロック連鎖モードの演算でＤＥＳアルゴリズムを使用すると、十分確立した順方向エラー伝播特性が立証される。このため、非暗号テキストで単一ビット程度の変化があると、ＭＡＣ内のすべてのビットが予定外に変更され、各ビットの確率が５０％になる恐れがある。長さがｋビットのＭＡＣを使用して、認証すべき関連メッセージとともにＭＡＣを送信し、その部分を宛先で受信されたメッセージについて再計算すると、送信したメッセージが改ざんされた場合に受信したＭＡＣが再計算したＭＡＣと一致する確率はわずか2^{-k}になる。ｋとして十分大きい値を選択すれば、この確率を所望の低い数値にすることができる。

【００３３】本発明の実施例では、暗号ブロック連鎖演算を使用して、メッセージ認証コード（ＭＡＣ）を生成する。暗号ブロック連鎖で使用するＤＥＳ演算は、特定の秘密キーを変換キーとして用いている。本明細書で論じる実施例では、秘密キーを用いてメッセージ認証コード（ＭＡＣ）を変換することで、メッセージ認証コード変換の結果として生成される認証タグが１人または複数の通信当事者を確実に認証できるようにしている。

【００３４】IEEE Communications Magazineの第２３巻、Ｎｏ．９に掲載された、R. R. Jueneman、S. M. Matyas、およびC. H. Meyerによる論文"Message Authentication"には、暗号ブロック連鎖演算に代わる方法が記載されている。

【００３５】認証プロトコルの応用例

本発明のプロトコルは、分散データ処理システムの１人または複数の通信パートナを認証するために分散データ処理システムで使用することができる。このような環境では、１台または複数のデータ処理装置が承認された媒介物の各種機能を実行する。図５は、本明細書に記載したプロトコルを実行できるようにプログラミング可能な分散データ処理システム８を示す。

【００３６】図５に示すように、分散データ処理システム８は、ローカル・エリア・ネットワーク（ＬＡＮ）１０および３２などの複数のネットワークを含んでもよいが、それぞれのネットワークは、複数の個別のコンピュータ１２および３０をそれぞれ含むことが好ましい。当然のことながら、当業者は、ホスト・コンピュータに連結した複数の高機能ワークステーションをそれぞれのネットワークに使用できることを認識できるだろう。このような分散データ処理システムでは一般的なように、それぞれの個人用コンピュータは、記憶装置１４またはプリンタ／出力装置１６あるいはその両方に連結してもよい。複数のユーザが同時にまたは連続してアクセスして処理することができる各種の「グループウェア」アプリケーションまたは文書を格納するために、本発明の方法およびシステムにより、１台または複数のこのような記憶装置１４を使用してもよい。さらに、従来技術により、グループウェア・アプリケーションおよび文書を含む、データ処理資源を管理するための１台または複数のシステムを含めてもよい。

【００３７】さらに図５を参照すると、分散データ処理システム８はメインフレーム・コンピュータ１８などの複数のメインフレーム・コンピュータも含むことができ、そのメインフレーム・コンピュータは好ましくは通信リンク２２によりローカル・エリア・ネットワーク（ＬＡＮ）１０に連結できるものであることが分かるだろう。メインフレーム・コンピュータ１８は、ローカル・エリア・ネットワーク（ＬＡＮ）１０用の遠隔記憶装置として機能できる記憶装置２０に連結することができ、通信制御装置２６および通信リンク３４を介してゲートウェイ・サーバ２８に連結することもできる。ゲートウェイ・サーバ２８は、ローカル・エリア・ネットワーク（ＬＡＮ）３２をローカル・エリア・ネットワーク（ＬＡＮ）１０にリンクする機能を果たす個別のコンピュータまたは高機能ワークステーション（ＩＷＳ）であることが好ましい。

【００３８】ローカル・エリア・ネットワーク（ＬＡＮ）３２およびローカル・エリア・ネットワーク（ＬＡ

N）１０に関連して前述した通り、複数のデータ・オブジェクト、アプリケーション・プログラム、およびデータ・ファイル、グループウェア・プログラムまたはグループウェア文書は、記憶装置２０内に格納し、このように格納したデータ・オブジェクトおよび文書用の資源マネージャまたはライブラリ・サービスとして、メインフレーム・コンピュータ１８で制御することができる。当業者は、このようなデータ・オブジェクト、アプリケーション・プログラム、データ・ファイル、グループウェア・アプリケーション、またはグループウェア文書に対する同時アクセスまたは連続アクセスと同時に、制限付きアクセスを許可して、グループ作業の有益な共同効果に対応することが望ましい場合が多いことを認識できるだろう。さらに、当業者は、メインフレーム・コンピュータ１８はローカル・エリア・ネットワーク（ＬＡＮ）１０から地理的にかなり離れた位置に配置でき、同様に、ローカル・エリア・ネットワーク（ＬＡＮ）１０はローカル・エリア・ネットワーク（ＬＡＮ）３２からかなり離れた位置に配置できることを認識できるだろう。つまり、ローカル・エリア・ネットワーク（ＬＡＮ）３２をカリフォルニアに配置する一方、ローカル・エリア・ネットワーク（ＬＡＮ）１０をテキサスに配置し、メインフレーム・コンピュータ１８をニューヨークに配置してもよい。

【００３９】その他の重要な利点

本発明は、通信パートナを認証すると同時に一時的なセッション・キーを通信パートナに分配するための安全かつ効率的な手段を提供し、もって「完璧で前向きな機密性」を提供する。つまり、敵対者が永続的な秘密キーを手に入れた場合、永続的な秘密キーを使用して分配した一時的なセッション・キーが被害を受けないことを意味する。言い換えれば、永続的なキーを知っているか所有していても、敵対者は、一時的なキーに関する利点が得られない。このため、敵対者が一時的なセッション・キーも知っているか所有していない限り、記録したセッションを「破壊」することができない。もう１つの重要な利点は、一方の特定の当事者から相当量の情報を得るために、敵対者が通信パートナを装い、連続してまたは順番に複数の通信パートナに関わり、その情報を使用してもう一方の通信当事者より優位に立つような「インタリーブ攻撃（interleaving attack）」から本発明のプロトコルが完全に保護されていることである。この種のインタリーブ攻撃は、通常、文献では「セッション」攻撃と呼ばれている。最も一般的な形態では、活動的な敵対者が２人の別々の通信パートナとの通信を開始し、一方のパートナから受信した通信を使用して、もう一方のパートナとのキー交換に入る。本発明は、この種の攻撃から完全に保護されている。

【００４０】

【発明の効果】本発明は、通信パートナを認証すると同時に一時的なセッション・キーを通信パートナに分配するための安全かつ効率的な手段を提供し、もって「完璧で前向きな機密性」を提供する。つまり、敵対者が永続的な秘密キーを手に入れた場合、永続的な秘密キーを使用して分配した一時的なセッション・キーが被害を受けないことを意味する。言い換えれば、永続的なキーを知っているか所有していても、敵対者は、一時的なキーに関する利点が得られない。このため、敵対者が一時的なセッション・キーも知っているか所有していない限り、記録したセッションを「破壊」することができない。もう１つの重要な利点は、一方の特定の当事者から相当量の情報を得るために、敵対者が通信パートナを装い、連続してまたは順番に複数の通信パートナに関わり、その情報を使用してもう一方の通信当事者より優位に立つような「インタリーブ攻撃（interleaving attack）」から本発明のプロトコルが完全に保護されていることである。この種のインタリーブ攻撃は、通常、文献では「セッション」攻撃と呼ばれている。最も一般的な形態では、活動的な敵対者が２人の別々の通信パートナとの通信を開始し、一方のパートナから受信した通信を使用して、もう一方のパートナとのキー交換に入る。本発明は、この種の攻撃から完全に保護されている。

【図面の簡単な説明】

【図１】先行技術による２当事者間のメッセージ認証を示す図である。

【図２】先行技術による従来のキー交換、すなわち、Diffie-Hellmanキー交換などの指数キー交換を示す図である。

【図３】BellovinおよびMerrittの教示による先行技術のキー交換を示す図である。

【図４】本発明の一実施例による２当事者間の相互認証動作を示す図である。

【図５】本発明の認証動作を実行するためにプログラミング可能な分散データ処理システムを示す図である。

【符号の説明】

Ａ　通信パートナ

Ｂ　通信パートナ

ａ　永続的な共用秘密キー

Ｔｅｘｔ１　テキスト・ストリング

Ｔｅｘｔ２　テキスト・ストリング

Ｔｅｘｔ３　テキスト・ストリング

E_a^1　変換

E_a^2　変換

h_a^1　変換

h_a^2　変換

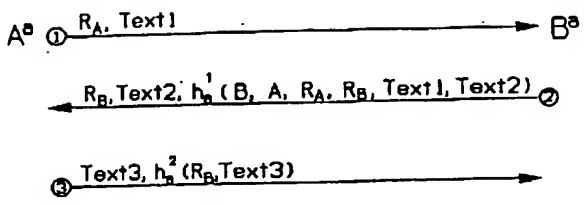
ｇ　基数

α　秘密キー

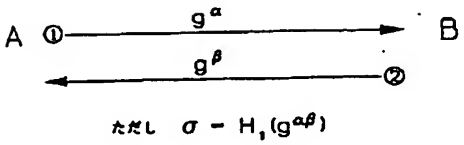
β　秘密キー

σ　一時的なセッション・キー

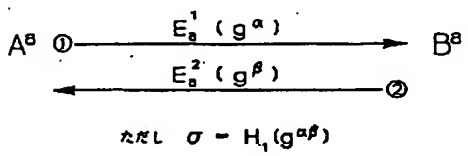
【図１】


A^B ① R_A, Text1
B^B
R_B, Text2, h_B^1 (B, A, R_A, R_B, Text1, Text2) ②
③ Text3, h_B^2 (R_B, Text3)

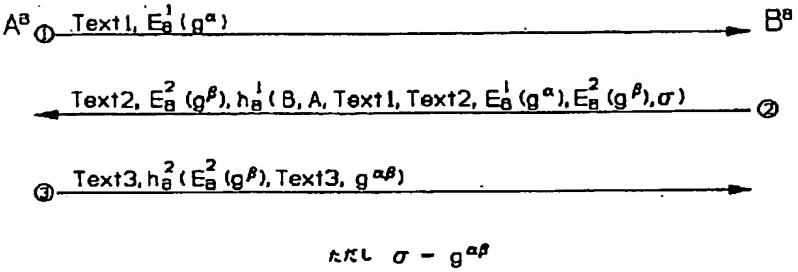
【図２】


A ① g^α
B
g^β ②
ただし　σ = H_1(g^αβ)

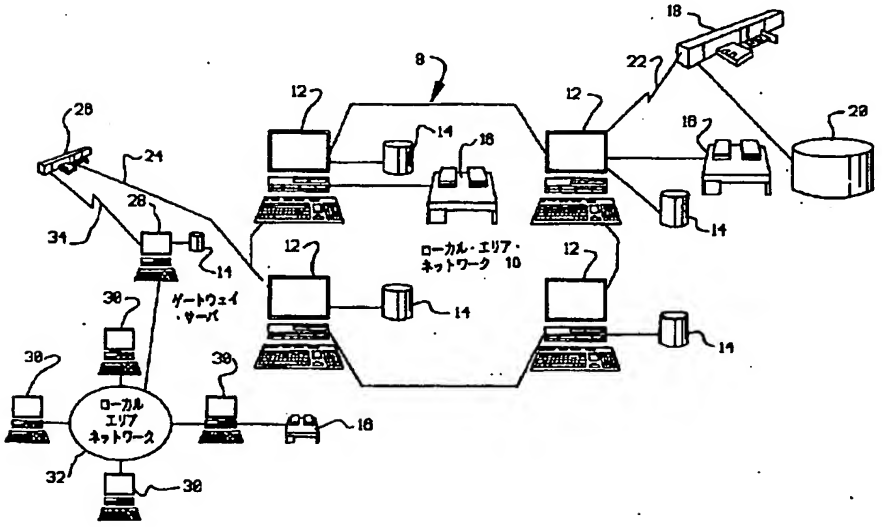
【図３】


A^B ① E_B^1 (g^α)
B^B
E_B^2 (g^β) ②
ただし　σ = H_1(g^αβ)

【図４】


A^B ① Text1, E_B^1 (g^α)
B^B
Text2, E_B^2 (g^β), h_B^1 (B, A, Text1, Text2, E_B^1 (g^α), E_B^2 (g^β), σ) ②
③ Text3, h_B^2 (E_B^2 (g^β), Text3, g^αβ)
ただし　σ = g^αβ

【図５】


8
12
14
16
18
20
22
24
26
28
30
32
34
ローカル・エリア・ネットワーク 10
ゲートウェイ・サーバ
ローカルエリアネットワーク

フロントページの続き

(56)参考文献　特開　平２－305039（ＪＰ，Ａ）
特開　平１－99159（ＪＰ，Ａ）
欧州特許出願公開535863（ＥＰ，Ａ２）
欧州特許出願公開223122（ＥＰ，Ａ２）
欧州特許出願公開661844（ＥＰ，Ａ２）
欧州特許出願公開307627（ＥＰ，Ａ１）

(58)調査した分野(Int.Cl.[6]，ＤＢ名)
H04L　9/00 - 9/38
G09C　1/00 - 5/00
G06F　15/00